CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

Founded 1984 ARI is the Official Newsletter of Computers Are Easy User Group

October 2023
Volume XXXIX Issue 10

Confirmed meeting dates

2023

Oct 28

Nov/Dec
Dec 9

Hybrid Board Room in person OR Zoom

:: ::

Check website for dates and meeting info

:: ::

Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL 60138

:: ::

****

PER GLENSIDE Library (Masks are optional)

INFORMATION for Saturday **October 28th** start time in person at Library Board Room is 9:30am or at home Zoom is 10:00am. This will be a hybrid meeting.

There will be a meeting invitation e-mail Thursday evening before the Saturday meeting.

Our **October 28** presentation will have various short video presentations about Cybersecurity

Make sure your software is up to date. Stay safe.

Dues for 2023 are due.
Mail dues to CAEUG, P.O. Box 3150,
Glen Ellyn, IL 60138

****

Thank you to all who have paid 2023 dues!

Table of Contents

Join CAEUG meeting in Library or from Home,
Stay Safe! Update information on our website at

https://www.CAEUG.net

CAEUG OFFICERS

President Carl Wallin

V.P. (Programs) Roger Kinzie
Secretary Position OPEN
Treasurer Kathy Groce
Newsletter Kathy Groce

Board Member
Frank Braman
Joanne Beauregard
Webmaster John Spizzirri
webmaster(at)caeug.net

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. The meeting(s) are not library sponsored Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline

Any member can volunteer to be on the Members Helpline.
Hardware problems, Win 7, Win 10, Linux and Virus Removal

- John Spizzirri

About DVD of the Month

Unfortunately, the DVD of the Month is no longer creating an income center for the club. August 2022 will be the last issue of the DVD. Starting in September, I will feature a review of a freeware program in the ARI... Some of these programs may be elaborate and complicated others may be very simple. I may include screen shots if that can be accommodated.

Lamp Post 262

October 2023
by John Spizzirri

The Brooks Falls brown bear fishing **(1)** has fallen off. The temperature is quite cold (just above freezing). Very few bears get in the water. Bears sit on rocks in the riffles **(2)** and scan the water for fish. The same is true at the Kat's River view **(3)**. River otters can be seen occasionally in the calmer waters. The live cams are turned off with highlight videos turned on more often.

1) **https://is.gd/5XSkeR**
2) **https://is.gd/8qsdz0**
3) **https://is.gd/BYn1NE**

October is Cybersecurity Awareness Month **(1, 2, 3)**. All these government agencies have the same advice; enabling multi-factor authentication **(MFA 4),** using, strong passwords and a password manager **(5)**, updating software **(6)**, recognizing and reporting phishing **(7, 8, 9)**.

1) **https://is.gd/bCSzKL**
2) **https://www.nist.gov/node/1102501**
3) **https://is.gd/HVwwsT**
4) **https://is.gd/PIxMLh**

Con't pg 3

5) **https://is.gd/zXca1l**
6) **https://staysafeonline.org/?p=14468**
7) **https://consumer.ftc.gov/node/77541**
8) **https://www.itgovernance.co.uk/blog/?p=31599**
9) **https://security.uchicago.edu/?p=1375**

On March 30, 1981, President of the United States Ronald Reagan was shot and wounded by John Hinckley Jr. **(1)**. In the hospital the medical personnel cut the President's clothing from his body. In doing so, they found and discarded a plastic card. That card was found in the President's shoe and held by the Federal Bureau of Investigation **(FBI 2)**. That card is known as the 'biscuit' and contains the codes to authorize a launch nuclear weapons. The briefcase that contains the communication device for the launch (called the football) is carried by a military officer who is with the president at all times. That safe guard is not enough to insure that a launch is intentional. The biscuit insures that the President is doing the communicating on the device (football) and is in his right mind as he must know the correct code to pick from the biscuit. That is what is known as multi-factor authentication **(MFA 3)**. The factors of MFA are something you know, something you are or something you have. Obviously, something you know is your user name and password. Something you are could be a fingerprint or facial recognition. Something you have could be a bank card, cell phone or security key. Having two of these three things are all that is needed for MFA to an account. Banks, insurance, Online investment accounts, wealth management accounts, etc. are all starting to require MFA to do business. Having two passwords or a password and a pin is not MFA. Two passwords is identical to a single password even if the passwords are different. Personally, I do not hold with fingerprint or facial recognition as both are so easily compromised **(4, 5, 6)**. Even with the advent of newer technology making facial recognition much more accurate, the system dependence on that accuracy is problematic (in my opinion). That leaves something you have like a card, key or phone. I personally do not like the idea of the phone as it requires a wireless connection to the cell system. That connection spys on the individual in hundreds of ways that cannot be measured. Therefore, I do not want to use a phone as a form of MFA. You, of course. may choose to use one. I prefer the bank card or a key like the Yubikey **(7)** or one of it competitors.

1) **https://is.gd/EnDdv1**
2) **https://www.fbi.gov/**
3) **https://is.gd/sDdlXK**
4) **https://is.gd/nFkAUC**
5) **https://is.gd/F5FtQd**
6) **https://wp.me/p9rsz1-6su**
7) **https://www.yubico.com/**

Malwarebytes **(1)** is a malware removal and protection software. It has a number of helpful pages on its web site with instruction on what to do to stay

safe on line. The first is a simple how to **(2)** that references two reports **(3, 4)**. Another page explains Quishing **(5)** which is phishing using QR codes **(6)**. Another page reported a data breach on 23andMe **(7)** that was first reported by Bleeping Computer **(8)** and updated by Tech Crunch **(9)**. The article explains what to do if you might be affected by this breach **(10)**. Another article explains what to do if you are affected by any data breach (**11)**.

1) https://www.malwarebytes.com/
2) https://is.gd/X3mkCB
3) https://is.gd/T2Jp9u
4) https://bityl.co/LtmN
5) https://is.gd/ZOu6De
6) https://is.gd/ch84Qh
7) https://www.23andme.com/
8) https://is.gd/Bm3VA3
9) https://techcrunch.com/?p=2616318
10) https://is.gd/SOlqrA
11) https://is.gd/URCBaL

To find out if your email address has been compromised by a data breach enter it in the Have I Been Pwned site **(1)** to get an immediate response. The Federal Trade Commission also has a site with information about what to do **(2)**.

1) https://haveibeenpwned.com/
2) https://consumer.ftc.gov/node/79791

Between you, me and the LampPost, that's all for now.

Personal Computer Security

By Dick Maybach, Brookdale Computer User Group
www.bcug.com
n2nd (at) att.net

Home users must manage three types of security:

- information security – protecting their information,
- application security – securing their applications against modification and misuse, and
- network security – preventing access to their network.

Only a small portion of your data, such as passwords and credit card numbers, is sensitive and needs special protection. For most, you are concerned only with recovery if lost, and here a good, well-tested backup discipline is the solution. It doesn't matter if the loss was because of hardware failure, operator error, or malicious software. Please note the "well-tested." If you haven't recently and successfully

Con't pg 5

restored data from a backup, you don't have a backup discipline, only a backup hope.

Sensitive data must be encrypted. I use KeePassXC, **https://keepassxc.org/**, for passwords, PINs, and financial access data, such as credit card and bank account numbers. The program stores these in an encrypted database, which I keep on my PC. If you keep it on the cloud, it will be available to all your devices with Internet access, but it's also more vulnerable to attack there. This means it needs a stronger password. A compatible Android app uses the same database as KeePassXC, which means the data is also safeguarded on your smartphone. The application also generates passwords of arbitrary complexity, making using a unique, strong password for each account easy. Other password programs have similar features. I use VeraCrypt, **https://www.veracrypt.fr/en/Home.html**, to encrypt files, directories, and storage media on my PC. I've seen reports that the EDS app allows access to VeraCrypt files on Android, but I haven't tested it.

Many financial institutions require two-factor authentication when you access your account. The most common is texting a one-time PIN to your cell phone after you log into your account with a username and password. You need both your password and the registered smartphone with them. Also, be careful when you travel that you can receive text messages in the countries you visit if you use credit cards.

Phishing attacks, where you get calls or messages asking you for sensitive information, are far more common than those through your PC. I get these almost every day, such as:

- "Your bank account has been locked; click this icon to unlock it,"
- "Your email storage is full; click this icon to free some,"
- "Your PC is infected with viruses; click here, and Microsoft will help you solve this,"
- "Amazon is about to ship you a new cell phone and charge your account; click this icon to prevent it," and
- "You owe money for past-due taxes; call the IRS at this number."

Usually, these are obvious scams, but occasionally you must do something. For example, your credit card company may contact you about a questionable purchase. In such cases, log into your account with the contact data in your password file or call the number on the back of the card. Also, never use a link in an email.

Many attacks occur when you contact disreputable websites. However, you can protect yourself by improving your browser's security.

- Chrome – **https://support.google.com/chrome/answer/10468685**
- Edge – **https://www.makeuseof.com/guide-to-security-settings-in-microsoft-edge/**
- Firefox – **https://trendoceans.com/firefox-privacy-and-security/**

Browsers are becoming more secure, which means keeping yours up to date is especially important. However, browsing can be dangerous; you feel safe because you

Con't pg 6

are comfortable in your own home, but you are poking through the back alleys of the world. If you have any concerns, use the Tor browser, **https://www.torproject.org/download/**, to protect yourself. Even better, install Tails Linux, **https://tails.boum.org/**, on a memory stick and explore from there rather than your usual operating system.

Be careful where you obtain software. Years ago, we would go to a tech store to buy a box with the storage medium and a manual, but the stores, boxes, media, and manuals have all but disappeared. We now download or install it directly from the Internet. I prefer to obtain mine from its developer's website after verifying that the URL is valid, and the developer is reputable. I've learned to avoid sites that warehouse many programs, as their downloads often include unwanted extras or malware. Check any download for malware before you run it, and if possible, test it on a secondary computer or virtual machine before you install it on your primary PC.

Keep all your software up to date, not just the operating system but all your applications. Many have bugs, some of which have security flaws, and anti-malware software may not protect you from someone exploiting these. Delete those applications you no longer use, as every one you have installed is a potential security risk. This also applies to smartphone apps.

Internet Service Providers (ISPs) are notorious for not updating the software in their terminal equipment. Unfortunately, your home network may not be secure, which can be problematic, especially if you have local file servers or other network devices. You can reduce your risk by installing your firewall between your home network and the ISP hardware, providing that you keep it updated and properly configured.

Some companies promote Internet-of-Things devices, such as video cameras that allow you to check on your home from work. Unfortunately, not all are designed for good security; others can also check on your home. Always change the usernames and passwords of such equipment from their defaults. Consider carefully whether the convenience of these is worth the risk, and purchase only those for which you can find thorough valid reviews.

Using a laptop on a public hotspot is much riskier than using one at home, as all your Internet data packets are visible to others using the same hotspot. Be sure to set your PC firewall for this environment and use a Tor browser or a VPN to encrypt your packets. Of course, encrypting sensitive data on a laptop is even more critical than on a home PC, as laptops frequently go missing. They are also more easily damaged, so they should be backed up, preferably by storing that data remotely. All this is even more true for smartphones.

Some PC users think that security begins and ends with anti-malware software, but reading the above should convince you otherwise. Such programs are helpful but address only a small portion of the risks.

Beware of Auto-Pays

Jim Cerny, 1st VP, Education Chair, and Forums Coordinator
Sarasota Technology Users Group
https://thestug.org/
jimcerny123 ** gmail.com

It sounds great, doesn't it? Don't bother sending us a check every month – put us on "auto-pay"! We will charge your credit card or get a payment from your bank account every month, so you don't have to do anything. If you make automatic payments, you can forget about paying us! And that's what they hope you do – forget that you ARE paying them every month!

Autopay is a convenient way to allow a company to receive regular payments from you without you having to do anything. Some examples of convenient auto-pay billing are for your internet services, TV cable providers, utility services, entertainment video providers, lawn maintenance, car insurance, home, and appliance insurance, tollway payments, and many others. In fact, almost ANY company would love to have you use autopay to pay them! And why not? If you owned a company, wouldn't you like all your customers to use autopay?

There is nothing wrong with the convenience of autopay, but it is often TOO convenient!

With autopay, you are giving a company permission to get their payment directly from your charge card or checking account. Doesn't this sound like a rather dangerous open-door policy? So here are my tips on the things to be careful about autopay:

1. ALWAYS check your charge card and bank statements CAREFULLY every month and make sure ALL charges are correct!!!

2. A company may be able to increase your auto-payment without notifying you. Does your contract with the company clearly state the regular payment amount?

3. If you lose your credit card or have a serious problem with your bank account, you may be given a new credit card or account number. Unfortunately, you must change all your auto-pays to the new account. This can be very troublesome, especially if a company tries to get payment from a closed account – they may cancel their service.
4. There is the danger of over-drafting your account or going over your charge account limit when paying your bills automatically. Therefore, you must ensure all your bills are always paid from accounts with sufficient funds.

5. You need to CANCEL any services you are no longer using. People have begun paying for a new service and forget to cancel the payments to the discontinued service they no longer need or want. Check your statements to ensure you are using what you are paying for.

Con't pg 8

4. Some companies may add additional charges for services or products, even if you did not order them.

Be careful to understand the advantages and dangers of using automatic payments. My bottom line: Carefully check your payments (checks, credit cards, etc.) every month to make sure your billing amounts and your payments are correct, and try not to use auto-pay unless you really need to.

Interesting Internet Finds
by Steve Costello
scostello ** sefcug.com

While going through more than 300 RSS feeds, I often encounter things that might interest other user group members.

The following are some items I found interesting in February.

Num Lock Will Ruin Your Day
https://cynmackley.com/2023/02/12/num-lock-will-ruin-your-day/

Con't pg 9

It is simple things like the Num Lock Key that can be frustrating. If you are like me, sometimes you try to use the number keypad and can't get numbers entered. Usually, I use the numbers on the upper row of the keyboard until I remember to check if the Num Lock Key is the problem.

Do You Really Need To Have Your VPN On All The Time?
https://www.howtogeek.com/866500/do-you-really-need-to-have-your-vpn-on-all-the-time/

This question comes up fairly often. This post gives pros and cons so you can decide about leaving the VPN on all the time. (Note: I keep the VPN on all the time on devices when I am traveling, while only when doing sensitive things like shopping or banking at home.)

Have You Made These Identity Theft Mistakes?
https://askbobrankin.com/have_you_made_these_identity_theft_mistakes.html

Bob Rankin goes over some common Identity Theft mistakes in this post. I read these posts to remind myself of best practices concerning Identity Theft prevention to ensure I am as safe as possible.

Which Should You Use On Your Smartphone?
https://www.online-tech-tips.com/smartphones/cellular-data-or-wi-fi-which-should-you-use-on-your-smartphone/

There is no best answer to this question, so I advise reading this article and making the best decision after having the facts. (Note: For me, it depends on the situation and the available speed.)

How Do I Keep My Email Address When I Change My ISP?
https://askleo.com/is_there_a_way_to_keep_my_email_address_when_i_change_my_isp/

Leo Notenboom explains ways to keep the same email address when changing ISPs. Unfortunately, there is not usually a way to do so if you use the ISP's issued email address, so things need to be set up beforehand.

****